



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10027206 A**(43) Date of publication of application: **27.01.98**

(51) Int. Cl.

**G06F 19/00**  
**G06F 17/60**  
**G06K 17/00**  
**G07D 9/00**  
**G07F 7/08**

(21) Application number: **08180394**(22) Date of filing: **10.07.96**(71) Applicant: **HITACHI LTD HITACHI VIDEO IND  
INF SYST INC**

(72) Inventor: **MATSUMOTO KENJI**  
**ITO SHIGEYUKI**  
**TAKAMI MINORU**  
**INOUE MASAYUKI**

(54) **ELECTRONIC PURSE ILLEGAL USE  
PREVENTING SYSTEM**

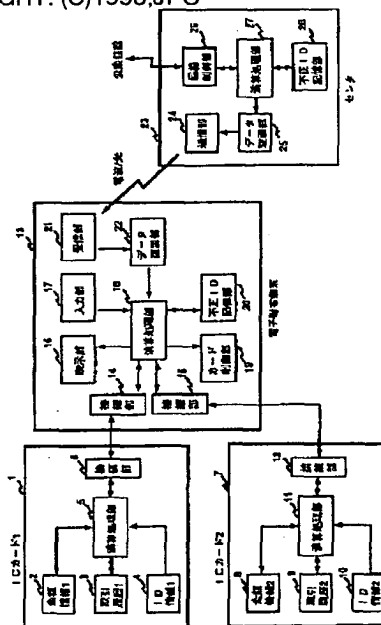
(57) Abstract:

**PROBLEM TO BE SOLVED:** To prevent the illegal use of an IC card even in an off-line processing for not performing circuit inquiry in a bank and a center by transmitting the ID number information of the IC card which is stolen or the like from the center and receiving an illegal ID number and checking the IC card on the side of an electronic purse terminal equipment.

**SOLUTION:** When an owner of the IC card inserts two sheets of the IC cards to the electronic purse terminal equipment 13 and depresses a remittance button in an input part 17, ID information 1 and the ID information 2 stored inside the IC card 1 and the IC card 2 are read out and supplied through connection parts 6, 12, 14 and 15 to an arithmetic processing part 18. In the arithmetic processing part 18, illegal ID number information registered in an illegal ID number storage part 20 inside the electronic purse terminal equipment 13 is read, whether or not the ID information 1 and the ID information 2 are registered as the illegal ID number information is checked, and when it is discriminated that it is the illegally used IC card, the IC card is

changed to a state incapable of taking out electronic money and forcedly ejected.

COPYRIGHT: (C)1998,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-27206

(43) 公開日 平成10年(1998) 1月27日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 19/00			G 0 6 F 15/30	3 3 0
17/60			G 0 6 K 17/00	L
G 0 6 K 17/00			G 0 7 D 9/00	4 6 1 Z
G 0 7 D 9/00	4 6 1		G 0 6 F 15/21	3 4 0 C
G 0 7 F 7/08			15/30	3 5 0

審査請求 未請求 請求項の数13 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願平8-180394

(22) 出願日 平成8年(1996) 7月10日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71) 出願人 000233136

株式会社日立画像情報システム

神奈川県横浜市戸塚区吉田町292番地

(72) 発明者 松本 健司

神奈川県横浜市戸塚区吉田町292番地株式  
会社日立製作所マルチメディアシステム開  
発本部内

(74) 代理人 弁理士 小川 勝男

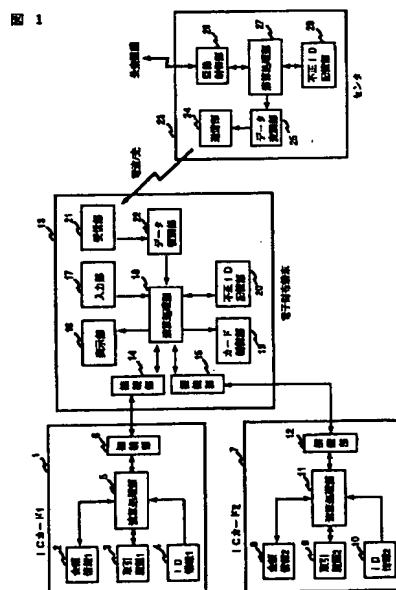
最終頁に続く

(54) 【発明の名称】 電子財布不正防止システム

(57) 【要約】

【課題】 電子財布システムでは、銀行や管理センタを経由しないオフライン処理であるため、盗難に遭ったICカードの不正使用を防止するのが困難である。

【解決手段】 センタから盗難に遭ったICカード1のID番号情報を電波や光を用いて無線で伝送し、端末装置でこの不正ID番号の受信とICカード1のチェックを行う。



## 【特許請求の範囲】

【請求項1】電子マネー情報とID情報を格納するICカードと、上記ICカードの情報を読み取り、書き込みを行うICカード読み書き手段と、上記ICカードの装着及び排出を制御するICカード制御手段と、不正ID情報を受信する受信手段と、上記不正ID情報を記録する記録手段と、上記ID情報と上記不正ID情報とを比較する演算処理手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記ID情報が上記不正ID情報として記録されている場合は、上記ICカードでの商取引を行わないことを特徴とする電子財布不正防止システム。

【請求項2】請求項1において、上記不正ID情報は電波や光を用いて伝送される電子財布不正防止システム。

【請求項3】電子マネー情報とID情報を格納するICカードと、上記ICカードの情報を読み取り、書き込みを行うICカード読み書き手段と、上記ICカードの装着及び排出を制御するICカード制御手段と、不正ID情報を受信する受信手段と、上記不正ID情報を記録する記録手段と、上記ID情報と上記不正ID情報とを比較する演算処理手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記ID情報が上記不正ID情報として記録されている場合は、上記ICカードでの商取引を行わないことを特徴とする電子財布不正防止システム。

【請求項4】請求項3において、上記不正ID情報は公衆回線網を通して伝送される電子財布不正防止システム。

【請求項5】電子マネー情報とID情報を格納するICカードと、上記ICカードの情報を読み取り、書き込みを行うICカード読み書き手段と、上記ICカードの装着及び排出を制御するICカード制御手段と、変調された不正ID情報を受信する受信手段と、上記不正ID情報を復調する復調手段と、上記復調された不正ID情報を記録する記録手段と、上記ID情報と上記不正ID情報とを比較する演算処理手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記ID情報が上記不正ID情報として記録されている場合は、上記ICカードでの商取引を行わないことを特徴とする電子財布不正防止システム。

【請求項6】請求項5において、上記不正ID情報は電波や光を用いて伝送される電子財布不正防止システム。

【請求項7】電子マネー情報とID情報を格納するICカードと、上記ICカードの情報を読み取り、書き込みを行うICカード読み書き手段と、上記ICカードの装着及び排出を制御するICカード制御手段と、変調された不正ID情報を受信する受信手段と、上記不正ID情報を復調する復調手段と、上記復調された不正ID情報を記録する記録手段と、上記ID情報と上記不正ID情報とを比較する演算処理手段とを有する電子財布端末装置

置とから構成され、上記演算処理手段の出力により、上記ID情報が上記不正ID情報として記録されている場合は、上記ICカードでの商取引を行わないことを特徴とする電子財布不正防止システム。

【請求項8】請求項7において、上記不正ID情報は公衆回線網を通して伝送される電子財布不正防止システム。

【請求項9】電子マネー情報を記録する手段と、ID情報を記録する手段と、信用情報を記録する手段と、上記信用情報の有効期限を判断する演算処理手段とを有するICカードと、上記ICカードの情報を読み取り、書き込みを行うICカード読み書き手段と、上記ICカードの装着及び排出を制御するICカード制御手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記信用情報が有効期限内の場合のみ、上記ICカードでの商取引を行うことを特徴とする電子財布不正防止システム。

【請求項10】電子マネー情報を記録する手段と、ID情報を記録する手段と、信用情報を記録する手段と、上記信用情報の有効期限を判断する演算処理手段とを有するICカードと、上記ICカードの情報を読み取り、書き込みを行うICカード読み書き手段と、上記ICカードの装着及び排出を制御するICカード制御手段と、上記信用情報を送受信する送受信手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記信用情報が有効期限内の場合のみ、上記ICカードでの商取引を行うことを特徴とする電子財布不正防止システム。

【請求項11】請求項10において、上記信用情報は電波や光を用いて伝送される電子財布不正防止システム。

【請求項12】電子マネー情報を記録する手段と、ID情報を記録する手段と、信用情報を記録する手段と、上記信用情報の有効期限を判断する演算処理手段とを有するICカードと、上記ICカードの情報を読み取り、書き込みを行うICカード読み書き手段と、上記ICカードの装着及び排出を制御するICカード制御手段と、上記信用情報を送受信する送受信手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記信用情報が有効期限内の場合のみ、上記ICカードでの商取引を行うことを特徴とする電子財布不正防止システム。

【請求項13】請求項12において、上記不正ID情報は公衆回線網を用いて伝送される電子財布不正防止システム。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子財布システムを用いて商取引を行う際に、盗難等に遭ったICカードのID番号情報を電波や光を用いて無線で流し、かつ、取引端末装置側でこの不正ID番号の受信及びチェック

を行うことにより、銀行等を経由しないオフライン処理においてもICカードの不正使用を防止することを可能とした電子財布不正防止システムに関する。

【0002】

【従来の技術】現在、商取引の際には、現金の代わりにクレジットカードによる支払いが普及しているが、支払いが後払い処理となるため、基本的には商取引の際に信用照会が必要となる。そのため、小売店側では銀行やセンタと公衆回線をつなぎ、オンライン処理で信用照会を行う。また、販売後も伝票処理等の手間や経費がかかるため、クレジットカードによる支払いは少額の買い物には向かない。

【0003】一方、クレジットカードによる支払いとは別に、特開平3-92966号公報に記載されているように、ICカードを使用した電子財布システムによる商取引の完全なキャッシュレス化も検討されている。これは、ICカード内のメモリに任意に指定された金額情報を書き込み、精算時にはICカードから必要な金額情報を送信することで、現金を用いずに商取引を完了させるシステムである。

【0004】

【発明が解決しようとする課題】この電子財布システムによる商取引が実現した場合、ICカード内の金額情報をやり取りするだけで支払いが終了するため、即時決済となり、小売店側では銀行やセンタへの信用照会及び伝票処理等が不要となる。このようなオフライン処理による支払いでは、クレジットカードのようなオンライン処理と比べて経費がかからないため、少額の買い物でも対応可能となる。

【0005】一方、電子財布システムでは、商取引時に銀行やセンタ等での信用照会がなされないため、ICカードが盗難に遭った場合や紛失した場合に不正使用を防止することが困難となる。そのため、ICカード自体に暗証番号で鍵をかけることにより、所有者以外は金額情報を取り出せなくすることも可能だが、鍵をかけ忘れた場合は不正使用を防止することは不可能であり、何らかの対策が必要である。

【0006】

【課題を解決するための手段】上記目的を達成するために、本発明では、電子マネー情報とID情報を格納するICカードと、上記ICカードの情報読み取り、書き込みを行うICカード読み書き手段と、上記ICカードの装着及び排出を制御するICカード制御手段と、変調された不正ID情報を受信する受信手段と、上記不正ID情報を復調する復調手段と、上記復調された不正ID情報を記録する記録手段と、上記ID情報と上記不正ID情報とを比較する演算処理手段とを有する電子財布端末装置とで構成する。

【0007】そして、上記演算処理手段の出力により、上記ID情報が上記不正ID情報として記録されている

場合は、上記ICカードでの商取引を行わないように制御を行う。

【0008】なお、上記不正ID情報は電波や光を用いてセンタから無線で伝送する場合や公衆回線網を通して伝送する場合が考えられる。

【0009】以上のように、本発明ではセンタから盗難等に遭ったICカードのID番号情報を送信し、かつ、電子財布端末装置側でこの不正ID番号の受信とICカードのチェックを行うことにより、銀行やセンタで信用照会を行わないオフライン処理においてもICカードの不正使用を防止することが可能となる。

【0010】

【発明の実施の形態】本発明の実施例を図1ないし図8を用いて説明する。

【0011】図1は本発明を用いた電子財布端末装置の一実施例であり、センタから盗難等に遭ったICカードのID番号情報が電波や光（例えば、赤外光など）を用いて無線で伝送され、電子財布端末装置側でこの不正ID番号のチェックを行う。

【0012】1はICカード1、2は金額情報記憶部1、3は取引履歴情報記憶部1、4はID情報記憶部1、5は演算処理部、6は接続部、7はICカード2、8は金額情報記憶部2、9は取引履歴情報記憶部2、10はID情報記憶部2、11は演算処理部、12は接続部、13は電子財布端末装置、14、15は接続部、16は表示部、17は入力部、18は演算処理部、19はカード制御部、20は不正ID情報記憶部、21は受信部、22はデータ復調部、23はセンタ、24は送信部、25はデータ変調部、26は回線制御部、27は演算処理部、28は不正ID記憶部である。

【0013】まず始めに、不正ID番号情報を送信するセンタ側の詳細を説明する。ICカードの所有者は、自分のICカードが盗難に遭った場合や紛失した場合に公衆回線を通してその旨をセンタに伝えるが、この情報は、回線制御部26を通して演算処理部27に供給される。演算処理部27では、このICカードのID番号を検索し、不正ID番号情報として不正ID番号情報記憶部28に登録する。その後、不正ID番号情報記憶部に登録されたその他の不正ID番号と共にデータ変調部25に変調され、送信部24から電波や赤外光などの光を用いて無線で伝送される。

【0014】次に、電子財布端末装置側の詳細を説明する。電子財布端末装置13には、電波や光で送信されたデータの受信部21があるが、受信された不正ID番号情報はデータ復調部22で復調後に演算処理部18に供給され、その後、不正ID番号情報記憶部20に登録される。この、不正ID番号情報の登録は、電子財布端末装置の電源が入れられた状態の時に自動的に行われるが、所有者がボタンを押すと登録されるような手動にしてもよい。

【0015】ここでは、図2を用いて、電子マネーにより個人間決済を行う場合を例に処理の流れを説明する。ICカード所有者が2枚のICカードを電子財布端末装置13に挿入して（S101）、入力部17で送金ボタンを押すと（S102）、ICカード1内に記憶されたID情報1が読み取られて、接続部6、14を通して演算処理部18に供給される（S103）。同様に、ICカード2内に記憶されたID情報2も接続部12、15を通して演算処理部18に供給される（S104）。その後、電子財布端末装置内の不正ID番号記憶部20に登録された不正ID番号情報が読み取られて、演算処理部18に供給される（S105）。

【0016】演算処理部18では、ID情報1及びID情報2が不正ID番号情報として登録されているかどうかのチェックを行い（S106）、不正に使用されているICカードであることが判明すると、そのICカードから電子マネーが取り出せない状態（以下、これをLock Out状態と呼ぶ）にICカードを変更して（S108）、カード制御部19により強制的にICカードを排出する（S110）。そのため、ICカードが盗難等に遭った際にカード所有者がセンタに申し出ることに  
より、そのICカードの不正使用は防止される。

【0017】一方、正常なICカードである場合は、演算処理部5、11で送金処理がなされて（S107）、金額情報記憶部1、2内の電子マネー残高が更新される。また、取引履歴情報記憶部1、2も同様に更新されて、取引履歴が記録される。ここで、送金処理を終了すると（S109）、ICカードが排出される（S110）。なお、表示部16には、決済する金額情報や処理の内容が表示される。

【0018】実施例では、電子財布端末装置を用いて電子マネーの決済を行う際にID番号のチェックを行うが、図3に示すようにICカードを電子財布端末に挿入するとすぐにID番号のチェックを行うようにしてもよい。この場合、不正なID番号であるとカードはすぐにLock Out状態になるが（S206）、正常なICカードの場合はICカードの残高照会や取引履歴の確認等の操作を行うことが可能となる（S205）。

【0019】以上のように、不正なID番号情報を電波や光を用いて無線で伝送することにより、電子財布端末装置を用いて決済を行うようなオフライン処理においてもICカードの不正使用を防止することが可能となる。この場合、不正ID番号情報の伝送方法としては、例えば専用のAM放送やFM文字多重放送などがあげられる。また、携帯電話と電子財布端末を組み合わせた装置では、無線による公衆回線で伝送することも可能である。

【0020】次に、図4を用いて本発明を用いたPOS端末の一実施例を説明する。POS端末等の場合、公衆回線を用いて売上金を銀行や本部に送金するため、不正

ID番号情報も公衆回線を用いて伝送することが可能となる。30はPOS端末、31は回線制御部、32は売上金額情報記憶部、33は売上履歴情報記憶部、34はセンタである。

【0021】この場合も、ICカードの盗難届けは公衆回線を通してセンタに送られるが、センタでは不正ID番号情報記憶部28に登録されたデータを回線制御部26を通して公衆回線で各POS端末に伝送する。また、伝送されたデータは、回線制御部31を介して各POS  
10 端末の不正ID番号情報記憶部20に登録される。

【0022】ここでは、図5を用いて処理の流れを説明する。ICカードの所有者がカードにより支払いを行う場合は、まず、ICカードをPOS端末30に挿入し（S301）、その後、買い物金額が表示部16に表示される（S302）。ICカードで支払いを行う場合は（S303）、ICカード内のID情報が読み取られて（S304）、接続部6、14を介して演算処理部18に供給される。その後、POS端末内の不正ID番号情報が読み取られて（S305）、同様に演算処理部18  
20 に供給される。

【0023】演算処理部18では、ID情報が不正番号情報として登録されているかどうかのチェックを行い（S306）、不正に使用されているICカードであることが判明すると、そのICカードをLock Out状態に変更して（S308）、カード制御部19により強制的にICカードを排出する（S313）。

【0024】一方、正常なICカードである場合は、次に、ICカード内の金額情報が読み取られて（S307）、買い物金額の支払いが可能かどうかのチェックがなされる（S309）。残高が足りない場合はその旨が表示部16に表示される（S311）と共に、ICカードが排出されて（S313）、取引が終了する。一方、支払いが可能な場合は、演算処理部5、18で送金処理がなされて、ICカード内の金額情報記憶部2が更新される（S310）と共に、取引履歴情報記憶部3も更新されて取引履歴が記録される。また、POS端末内の売上金額情報記憶部32が更新され（S312）、さらに、売上履歴情報記憶部33も更新された後に、ICカードが排出される（S313）。

【0025】以上により、公衆回線で伝送された不正ID番号情報がPOS端末でチェックされるため、ICカードの不正使用を防止することができる。

【0026】次に、図6を用いて、不正ID番号データの変調部及び復調部を説明する。不正ID番号情報を無線で伝送する場合、データの偽造を防ぐために何らかの暗号化が必要となる。そこで、本発明では、図6に示すように暗号鍵により不正ID番号情報の暗号化を行う一例を説明する。

【0027】まず、データ変調部25では、演算処理部から供給された不正ID番号情報をID暗号化部45で

暗号化する。この場合、ID暗号化部鍵情報記憶部48に格納されたID暗号化部鍵により、あらかじめ定められた規則で暗号化を行う。また、このID暗号化部鍵はID暗号化部鍵情報の暗号化部47で暗号化されるが、この場合も暗号化の際には暗号鍵記憶部46に格納された暗号鍵により、一定の規則で暗号化される。これらの暗号化されたデータは、送信部24から電波や光などの無線で送信される。

【0028】一方、無線で送信されたデータは受信部21で受信されて、データ復調部22に供給される。暗号化されたデータの中で、ID暗号化部鍵は復号化部50で復号化されるが、復号化部50での処理の際には暗号鍵記憶部51に格納された暗号鍵により定められた規則で復号化される。なお、この暗号鍵はセンタにより一括管理されている。そのため、センタから送信された正式なデータを受信した場合のみ、復号化部50でID暗号化部鍵を復号化することができる。その後、このID暗号化部鍵により、不正ID番号情報がID復号化部49で復号化される。

【0029】以上により、センタから送られてきた正式な不正ID番号情報のみが再生されるので、データの偽造を防ぐことが可能となる。

【0030】次に、ICカード自体に信用情報を登録する例を説明する。実施例では、センタから送られてくる不正ID番号情報を端末側でチェックすることでICカードの不正使用を防止したが、ICカード自体に信用情報を定期的に登録することにより不正防止を行うことも可能である。図7では、ICカード35がPOS端末36に挿入されるとICカードのID情報が読み取られて、POS端末の回線制御部31を介してセンタ34に公衆回線で送られる。センタではこのID番号が不正ID番号記憶部28に登録されていないかどうかのチェックを行い、不正なものではないことを確認すると信用情報が公衆回線を通してPOS端末36に送信され、その後、この信用情報がICカード35内の信用情報記憶部37に格納される。ここで、不正なID番号の場合は、信用情報記憶部37内のデータは更新されない。

【0031】ICカードを用いて商取引を行う場合、決済時にICカードに登録された信用情報のチェックを演算処理部5で行い、信用情報が正しく登録されていないカードでは決済が行えないようにすることで不正使用を防止することができる。この場合、信用情報には期限を設けて、かつ、ICカードの所有者が定期的に信用情報の更新を行うようにすれば、不正なICカードでは信用情報が更新されないため、決済を行うことができない。

【0032】なお、この信用情報の登録は、公衆回線でセンタと接続された端末であれば可能であり、POS端末以外でも銀行のATM端末等で行うこともできる。この場合、信用情報の更新は、POS端末やATM端末にアクセス時に自動的に行われるが、所有者が選択すると

行われるように制御してもよい。また、電波や光等の無線を用いてセンタと情報のやり取りを行ってもよい。

【0033】ここで、図8に示すように、ICカード38内に信用情報チェック部39を内蔵させて、信用情報を専用回路でチェックさせることも可能である。この場合、信用情報チェック部39では、信用情報と共にICカード内の取引履歴や金額情報などのデータもチェックして、ICカードが真に正常なものである場合のみ取引決済を行うように制御することも可能である。また、チェック結果に基づき、信用情報記憶部37のデータを再度更新するようにしてもよい。

【0034】なお、信用情報チェック部はPOS端末やATM側に持たせることも可能である。この場合、信用情報チェック部を不正に使用することも考えられるため、センタからの指令でのみ動作を行うように制御することで安全性を高めることができる。

【0035】以上のように、ICカード自体に有効期限付きの信用情報データを持たせて、所有者がオンラインで定期的に更新することにより、オフライン処理である電子財布端末を用いた場合でも不正ICカードの使用を防止することができる。

【0036】

【発明の効果】本発明では、センタから盗難等に遭ったICカードのID番号情報を電波や光を用いて無線で伝送し、かつ、電子財布端末盗難等でこの不正ID番号の受信とICカードのチェックを行うことにより、銀行やセンタで信用照会を行わないオフライン処理においてもICカードの不正使用を防止することが可能となる。また、センタから不正ID番号を公衆回線で伝送し、POS端末等で不正使用のチェックを行うことも可能である。さらに、ICカード自体に信用情報を持たせて、決済時にこの信用情報をチェックすることで不正防止をすることもできる。この場合、信用情報に期限を設けて、かつ、ICカード所有者がオンラインで定期的に信用情報を更新することにより、不正なICカードは信用情報の更新ができないため、決済を行うことができない。

【図面の簡単な説明】

【図1】本発明を用いた電子財布端末装置の一実施例のブロック図。

【図2】本発明を用いた電子財布端末装置での操作のフローチャート。

【図3】本発明を用いた電子財布端末装置での操作のフローチャート。

【図4】本発明を用いたPOS端末の一実施例のブロック図

【図5】本発明を用いたPOS端末での操作のフローチャート。

【図6】本発明を用いた不正ID番号データの変調部及び復調部の一実施例のブロック図。

【図7】本発明を用いたPOS端末の第二の実施例のブ

ロック図。

【図8】本発明を用いたPOS端末の第三の実施例のブロック図。

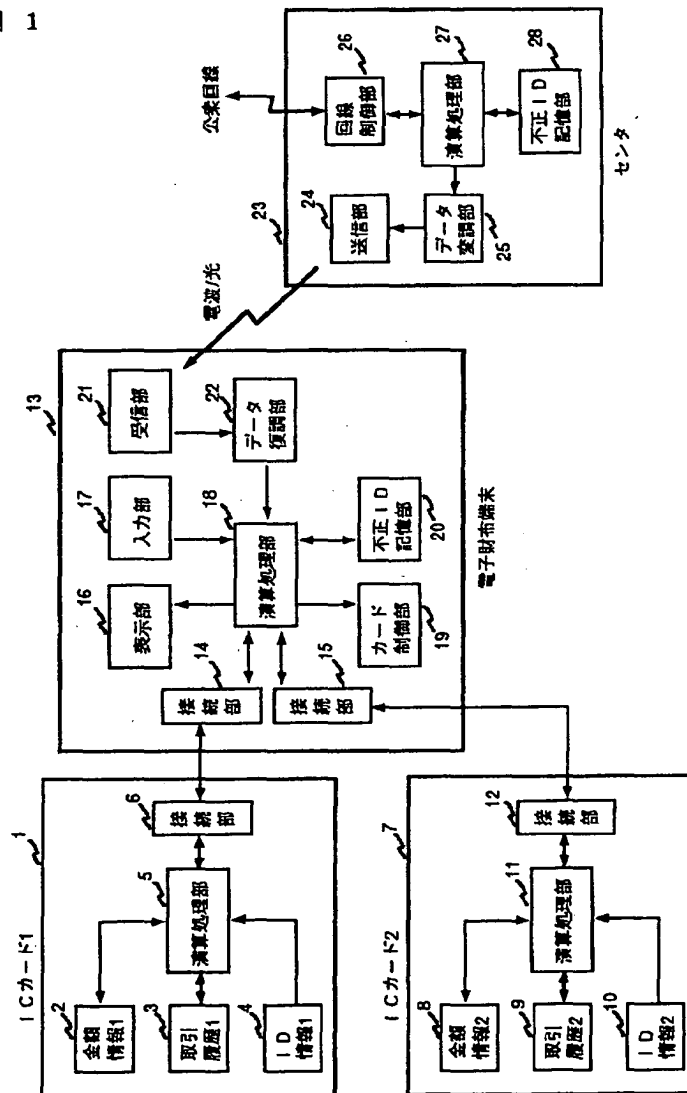
【符号の説明】

1…ICカード、2…金額情報記憶部、3…取引履歴情報記憶部、4…ID情報記憶部、5…演算処理部、6…接続部、7…ICカード、8…金額情報記憶部、9…取

引履歴情報記憶部、10…ID情報記憶部、11…演算処理部、12…接続部、13…電子財布端末、14、15…接続部、16…表示部、17…入力部、18…演算処理部、19…カード制御部、20…不正ID記憶部、21…受信部、22…データ復調部、23…センタ、24…送信部、25…データ変調部、26…回線制御部、27…演算処理部、28…不正ID記憶部。

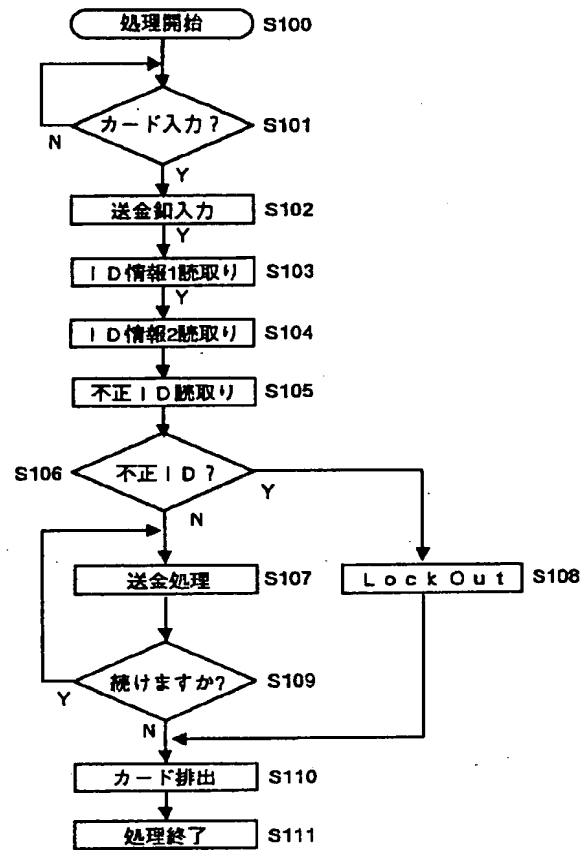
【図1】

図 1



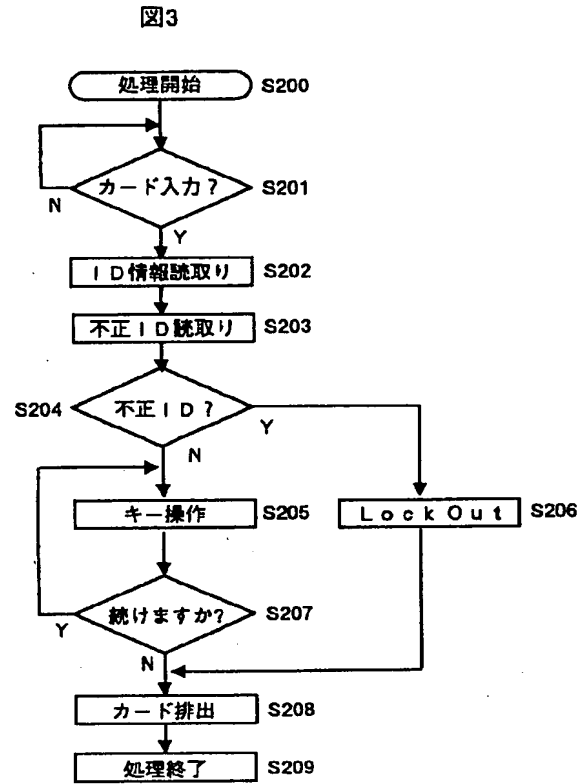
【図2】

図2



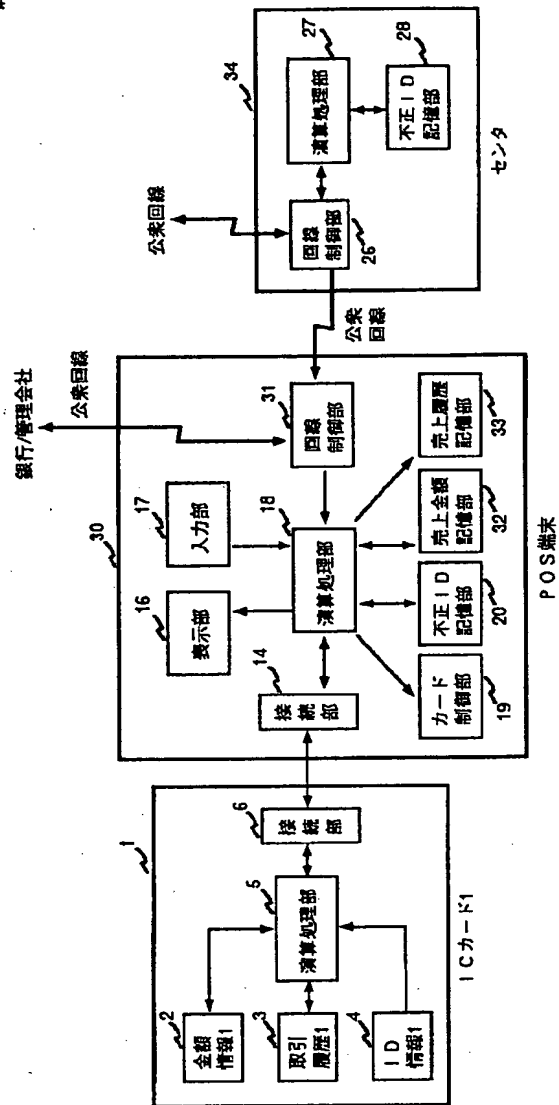


【図3】

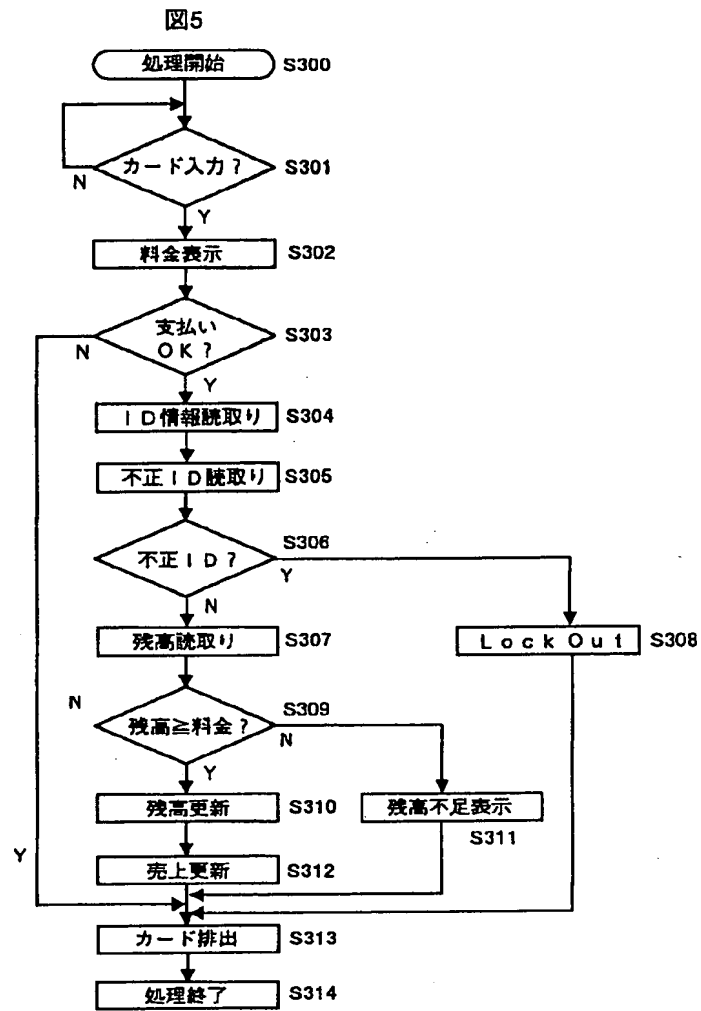


【図4】

図 4

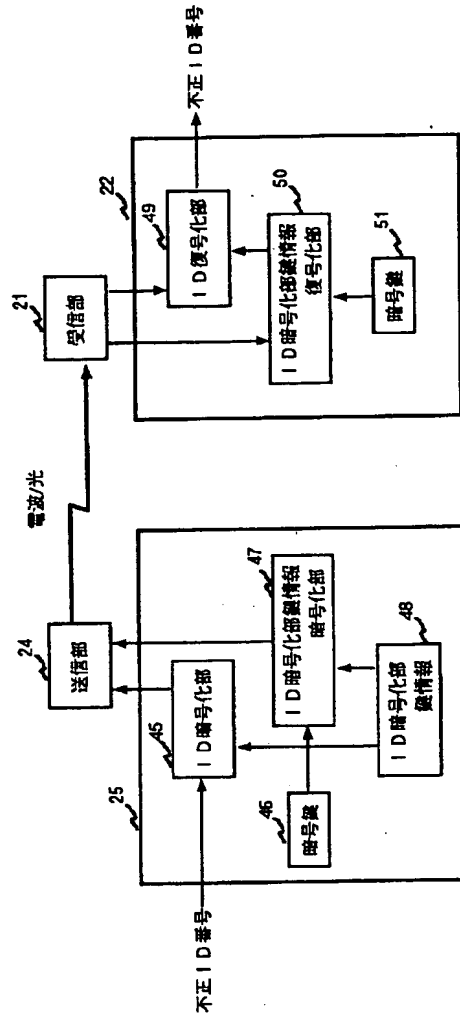


【図5】



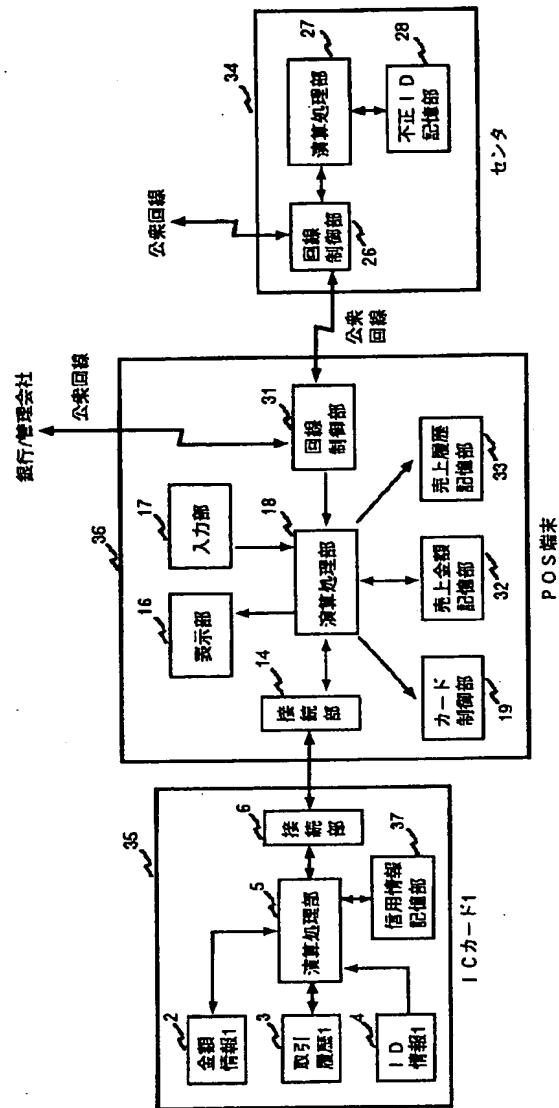
【図6】

図 6



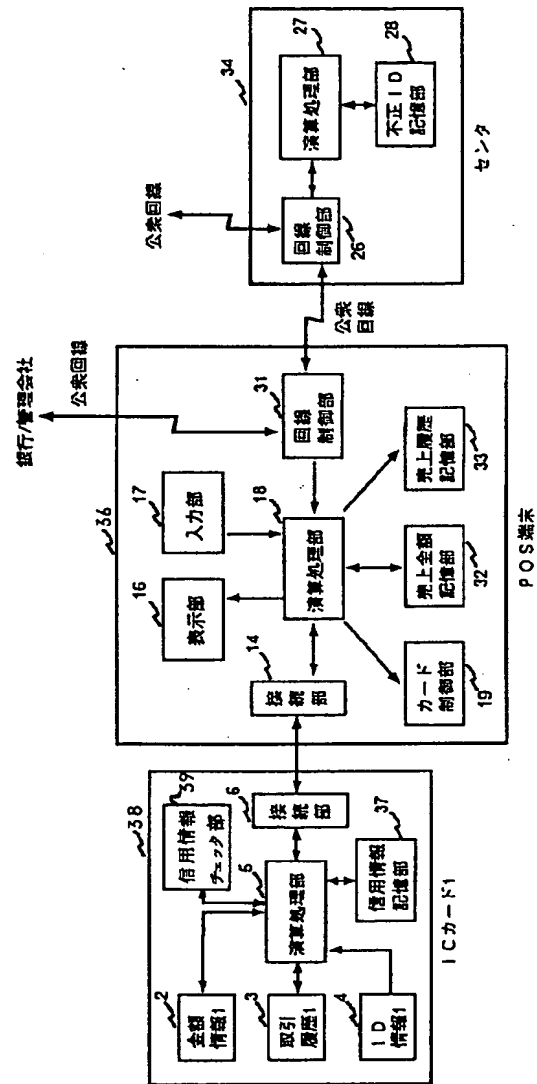
【図7】

図 7



【図8】

図 8



フロントページの続き

(51)Int.Cl.6

識別記号 庁内整理番号

FI  
G07F 7/08

技術表示箇所

Z

(72)発明者 伊藤 滋行  
神奈川県横浜市戸塚区吉田町292番地株式  
会社日立製作所マルチメディアシステム開  
発本部内

(72)発明者 高見 穰  
神奈川県横浜市戸塚区吉田町292番地株式  
会社日立製作所マルチメディアシステム開  
発本部内

(72)発明者 井上 雅之  
神奈川県横浜市戸塚区吉田町292番地株式  
会社日立画像情報システム内